Transforming the Internet Service Provider's (ISP's) Role in Cyber Security

Michael J. Miller, CISSP
Vice President, Federal Sector
michael.j.miller@globalcrossing.com
(703) 464-3318

Global Crossing®
Think Ahead

Learning Objectives

- Cyber security at ISP level will improve the level of protection for customers
- Centrality to the Internet is key for detection and prevention
- Advanced perimeter security measures can be simplified by deploying cyber security within the ISP cloud
- Analysis is essential in identifying advanced persistent threats that often go undetected by traditional security measures
- ISP's can offer a new class of "Assured" services that they can provide to their customers, protecting the communication path

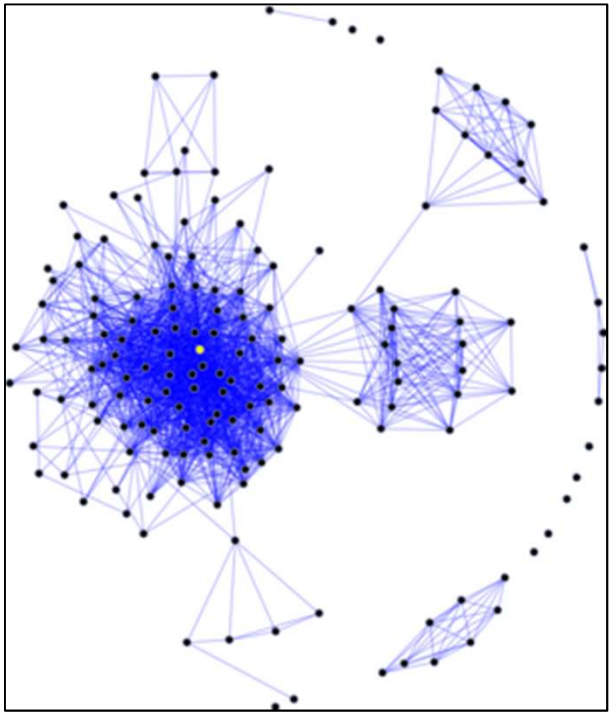
Agenda

- Internet Centrality
- Global Crossing's Worldwide Network
- Threat Landscape
- The Problem
- Today's Internet
- Determining IP Reputation
- Tomorrow's Internet
- Transforming the ISP's role in Cyber Security
- Benefits of Security in the "Cloud"
- The Availability Theory

Internet Centrality

Cyber Security continues to be a complex problem that needs to be addressed throughout the entire communication path. Carriers have a unique role in the protection of this path based on their centrality to the Internet.

By default, an Internet Service Provider (ISP) has considerable influence and insight due to the number of nodes and connections. A global ISP increases this value significantly.



An example of a social network diagram.
Source: http://en.wikipedia.org/wiki/Social_network

About Global Crossing's Worldwide Network

Worldwide Presence:

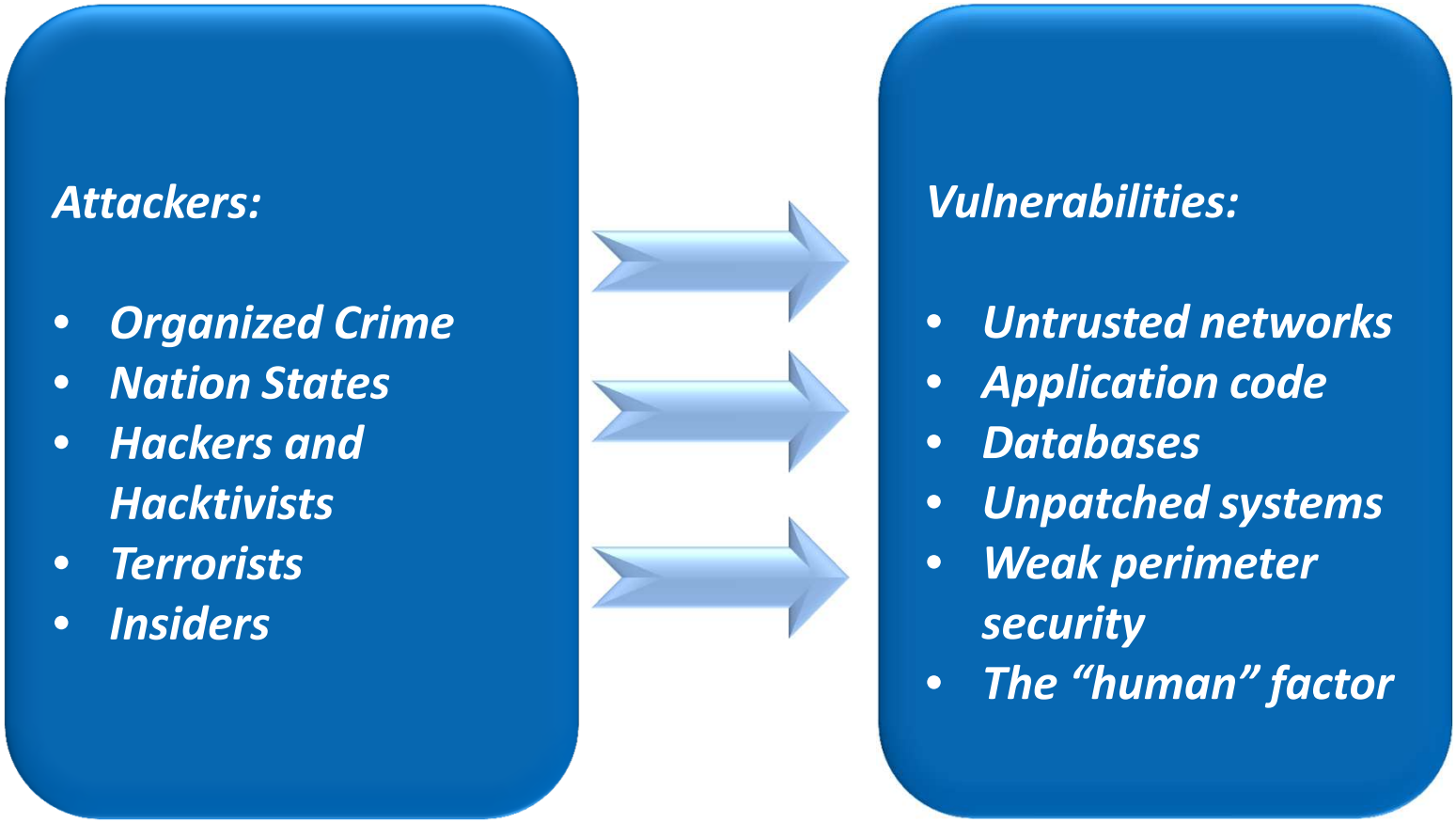
- 2nd largest customer base Global ISP
- 6 continents
- 190 countries
- 62 US states or Canadian provinces
- 36 US Metro areas

renesys

The Network:

- First carrier to deploy global MPLS network
- Transporting 23.4 PB IP traffic carried on average per day
- Over 100,000 route miles of optical cable globally
- 2nd largest carrier of global internet traffic
- Dual stack IPv4 / IPv6 core network

Threat Landscape



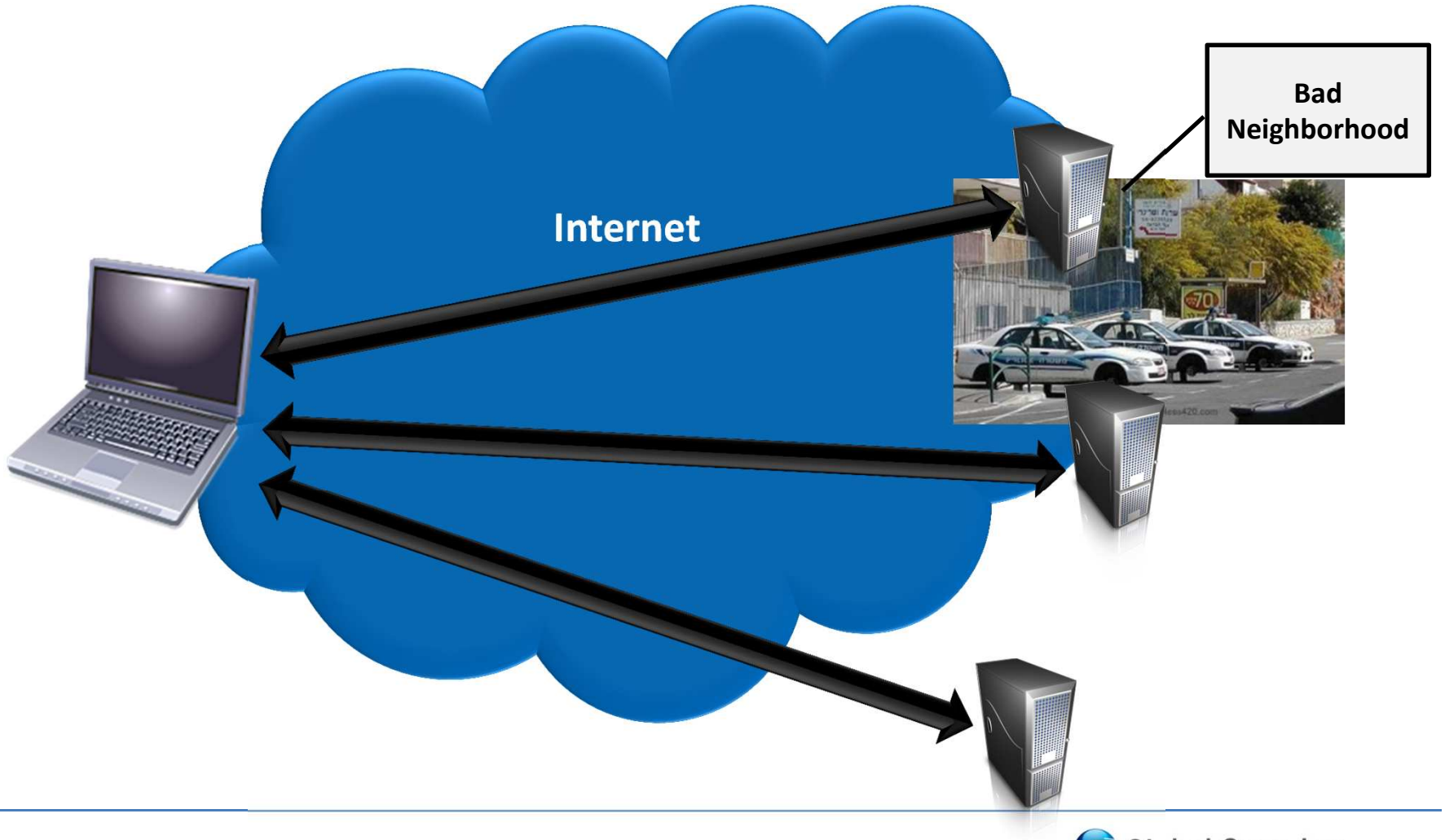
The Problem

The Internet is unsafe!

The Challenge

- It’s difficult to manage and secure your perimeter against a constantly changing threat landscape
- There is a tremendous amount of data with limited resources to analyze the data
- Technology and users are dynamic and they will find the point of least resistance
- Networks are fluid
- One bad actor can impact many targets (One to Many)
- Lack of understanding the problem at all levels…

Today's Internet



Global Crossing
Think Ahead

Today's Approach

Every entity is dealing with the cyber threat on an individual basis.

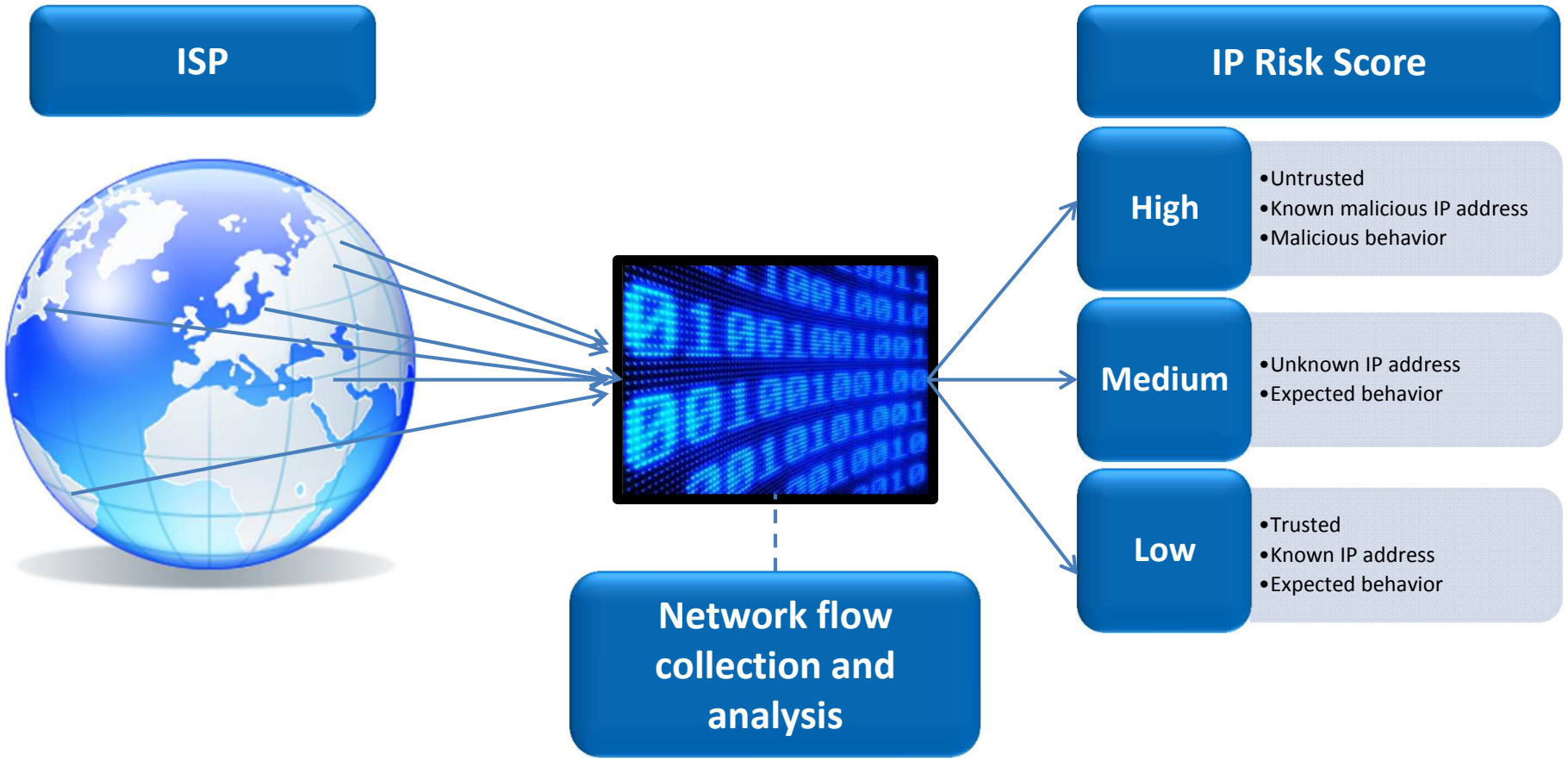
Concept #1

Utilize information that is available today (network flow data) to start to develop the situational awareness of who you are communicating with and who is trying to communicate with you.

Analyze your network flow data to determine if your data is going to known “bad neighborhoods”.

Implement security measures to prevent your traffic from going to “bad neighborhoods”.

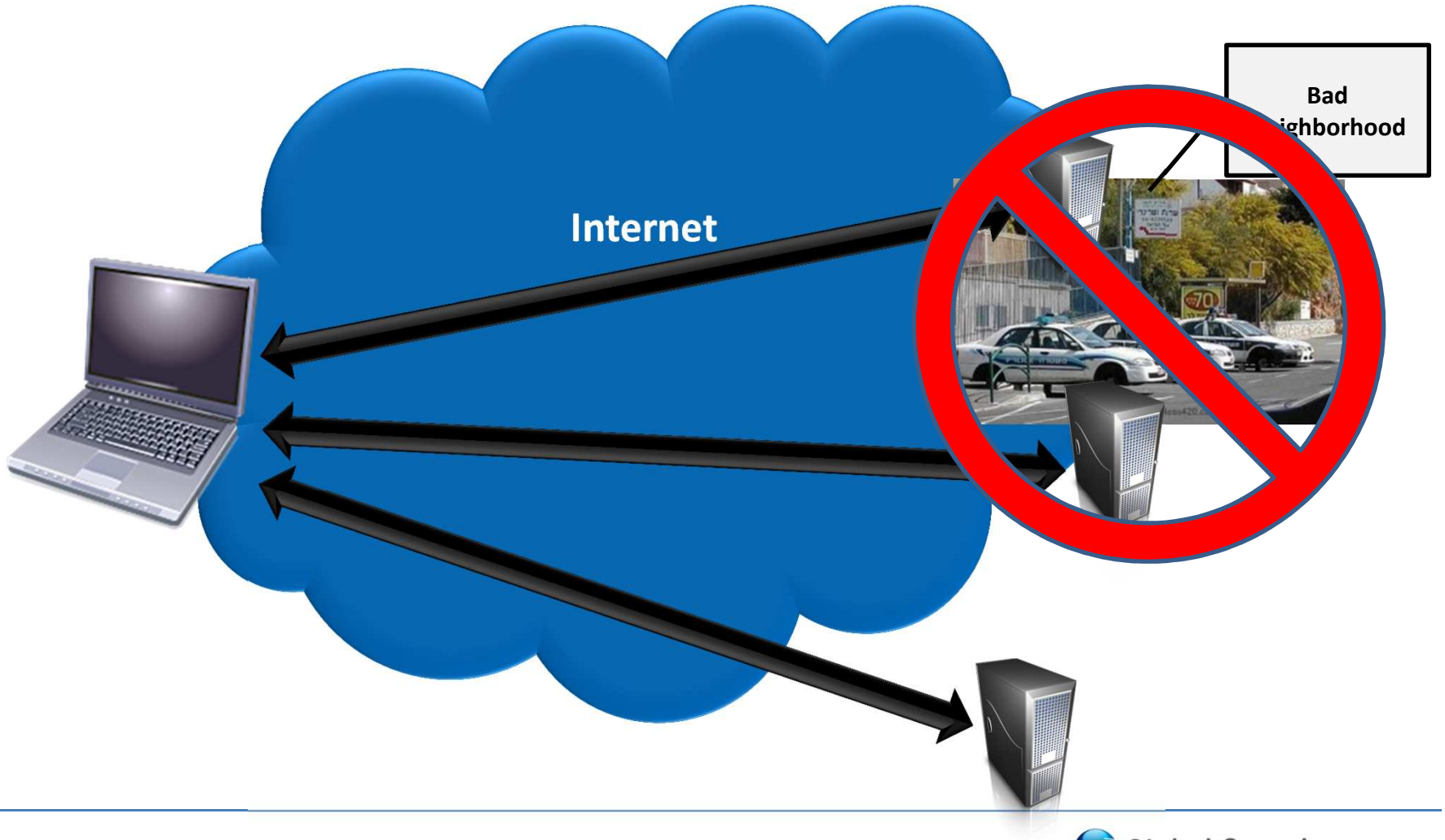
Determining IP Reputation



How does this help solve the problem?

- Centralized vs. decentralized analysis
- Aggregation of ISP network flow data can identify threats that would not have been detected at the Enterprise level
- Greater economies of scale and resources can be applied, increasing the effectiveness and lowering the cost
- IP reputation data can be used to determine the potential risk level that an Enterprise can evaluate and determine the acceptable risk tolerance
- Removing the known “bad neighborhoods” reduces the dataset that Enterprises need to focus on

Tomorrow's Internet



Global Crossing
Think Ahead

Concept #2

Advanced perimeter security measures can be simplified by deploying cyber security within the ISP cloud.

Benefits of Security in the “Cloud”

- Situational Awareness
- Attack Attribution
- Analysis on Massive Data Scales
- Situational Understanding at Multiple Timescales
- Dedicated Resources
- Technology Refresh
- Risk Mitigation
- Flexible Services
- Improved Availability

Concept #3

ISP’s can offer a new class of “Assured” services that they can provide to their customers, protecting the communication path.

New “class of service”

“Assured” services applies a class of service ranking on Internet traffic based on trusted zones or address space.

The trusted zones can be determined by analyzing the “bad neighborhoods”.

Techniques for “Assured” services

- Whitelists
- Blacklists
- IP reputation - real time decisions

Concept #4

The CIA security model should be revisited to focus on “Availability”!

Transforming the ISP's role in Cyber Security

It's about protection

- *Availability*
- *Confidentiality*
- *Integrity*

The Availability Theory

Improved Security = Improved Quality = Improved Availability

Measures taken to improve the ***security*** of your network, and to reduce your organizations exposure to “bad Internet neighborhoods”, will improve the ***quality*** of the traffic on your organization’s network. As quality of the traffic improves, your organization will see less malicious traffic and less potential threats against the network, resulting in better network ***availability***.

Summary

- The problem is complicated
- We need to rethink our strategies around security
- Individual Enterprises are stressing their resources and capital to address similar threats
- Identifying “bad neighborhoods’” can reduce your risk and improve security
- Your ISP should be part of your defense-in-depth strategy
- Availability is critical

THANK YOU

For more information visit:

http://www.globalcrossing.com/federal